BERNADETTE PERRIN-RIOU

Plongeants d'extensions galoisiennes

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 19, n° 2 (1977-1978), exp. n° 38, p. 1-7

<http://www.numdam.org/item?id=SDPP_1977-1978__19_2_A12_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
19e année, 1977/78, n° 38, 7 p.

24 avril 1978

PLONGEMENTS D'EXTENSIONS GALOISIENNES

par Bernadette PERRIN-RIOU

Soit K/k une extension galoisienne de groupe de Galois G et E une extension de G. On se demande s'il existe une surextension N/k contenant K de groupe de Galois isomorphe à E et telle que la restriction des automorphismes corresponde au passage au quotient $E \longrightarrow G$. Si une telle surextension existe, on dit que le problème de plongement relatif à E et à K/k a une solution.

On s'est occupé du cas où G est un groupe diédral d'ordre 2^{k+1}, et où E est un groupe diédral ou quaternionien d'ordre 2^{r+k+1}. Le noyau de l'extension est alors un groupe cyclique A d'ordre 2^r. Ces groupes sont définis par générateurs et relations de la manière suivante :

$$G = \langle x\ ,\ y\ ,\ x^{2^k} = 1\ ,\ y^2 = 1\ ,\ yxy^{-1} = x^{-1} \rangle\ ,$$

$$E = \langle \sigma\ ,\ \tau\ ,\ \sigma^{2^{r+k-1}} = 1\ ,\ \tau^2 = \sigma^2\ \ (\text{ou}\ \ 1\ )\ ,\ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle\ .$$

Certains cas de ce problème ont déjà été résolus. DAMEY et PAYAN [1] ont étudié le cas du plongement d'une extension de Klein dans une extension diédrale ou quaternionienne d'ordre 8, le corps de base étant le corps $\underset{\sim}{Q}$ des rationnels. Ils utilisent la théorie de Kummer, ce qui leur permet de construire explicitement l'extension $N/\underset{\sim}{Q}$. GILLARD [4] a étudié le même problème sur un corps quelconque dans lequel il n'existe qu'une seule place au-dessus de 2 non décomposée dans K/k. MARTINET et DAMEY [2] ont étudié le plongement d'une extension quadratique dans une extension quaternionienne d'ordre quelconque. Enfin, HALTER-KOCH [5] a étudié le cas du plongement d'une extension diédrale dans une extension diédrale ou quaternionienne d'ordre une puissance de 2, dans le cas où le corps de base est $\underset{\sim}{Q}$ en construisant un caractère sur les classes d'idèles d'un corps quadratique, ce qu'il a d'ailleurs exposé dans [5].

1. Méthode utilisée.

Ce qui suit est un court rappel de la méthode générale qui sera utilisée dans le cas particulier étudié ([8], [9]).

On suppose que A est un groupe abélien. L'extension E de G par A est décrite par l'action de G sur A et par un élément ϵ de $H^2(G\ ,\ A)$. Soit $\bar{k}$ une clôture séparable de k et $\bar{G}$ le groupe de Galois de $\bar{k}/k$. Pour que le problème de plongement relatif à E et K/k ait une solution, il faut que l'image de ϵ par inflation dans $H^2(\bar{G}\ ,\ A)$ soit nulle (HOECHSMANN). Cette condition est suffisante dans le cas où k est un corps de nombres, ou dans le cas où E et G sont deux groupes de même rang. Cette condition peut être transcrite à l'aide des théorèmes de dualité locale et globale. Dans le cas local (cela a été fait par NEUKIRCH), la condition est que, pour tout caractère χ de $A' = \mathrm{Hom}(A\ ,\ \bar{K}^*)$ défini sur k , c'est-à-dire invariant par $\bar{G}$, on ait $\chi^*(\varepsilon) = 0$. Dans le cas global (cela a été fait par POITOU), la condition est que s'annulent dans $H^2(G\ ,\ C(K))$ toutes les images $\chi^*(\varepsilon)$, où χ est un caractère de A dans le groupe $\mathfrak{C}$ des classes d'idèles de $\bar{K}$, défini sur k . D'autre part, si on choisit un prolongement de toute place v de k jusqu'à $\bar{K}$, et si on appelle G_v et $\bar{G}_v$ les sous-groupes de décomposition relatifs à v , on appelle condition locale la condition d'annulation de l'image de ε par restriction, puis inflation dans $H^2(\bar{G}_v\ ,\ A)$:

$$H^2(G\ ,\ A) \xrightarrow{\text{res}} H^2(G_v\ ,\ A) \xrightarrow{\text{inf}} H^2(\bar{G}_v\ ,\ A)\ ,$$

ce qui est équivalent à la condition d'annulation de tous les $\chi_v^*(\varepsilon)$, où χ_v décrit les caractères de A dans $\bar{K}_v$ définis sur k_v . Ces conditions locales sont équivalentes à la condition d'annulation de $\chi^*(\varepsilon)$, pour tout élément χ de $\mathrm{Hom}_k(A\ ,\ \mathfrak{C})$ appartenant à l'image de π^* :

$$\pi^* : \mathrm{Hom}_k(A\ ,\ \mathfrak{J}) \longrightarrow \mathrm{Hom}_k(A\ ,\ \mathfrak{C})$$

($\mathfrak{J}$ désigne le groupe des idèles de $\bar{K}$). Si on suppose les conditions locales vérifiées, il suffit d'écrire l'annulation de $\chi^*(\varepsilon)$, pour tout χ appartenant au conoyau de π^* (conditions globales). Ce conoyau est fini. Dans le cas où A est cyclique d'ordre une puissance de p , qui est le cas qui nous intéresse, le conoyau contient 1 ou 2 éléments. Il en contient 2 si, et seulement si, A est d'ordre 2^r , et si le groupe de Galois de $k(A')/k$ est non cyclique et distinct de tous ses sous-groupes de décomposition. On peut décrire explicitement l'élément non nul de la manière suivante. Le groupe de Galois de $k(A')/k$ peut être considéré comme un sous-groupe de $(\underset{\sim}{Z}/2^r\ \underset{\sim}{Z})^*$ engendré par β et α^{2^s} ($\beta = -1$, $\alpha = 5$, $s < r-2$) . Soit k' le corps laissé fixe par α^{2^s}, $k(+)$ le corps laissé fixe par β et $\alpha^{2^{s+1}}$, $k(-)$ le corps laissé fixe par $\beta\alpha^{2^s}$. Soit λ_j un élément d'ordre 2^{j+2} de A' vérifiant $\lambda_{j+1}^2 = \lambda_j$. On calcule le caractère $\underline{\psi}$ du conoyau dans $\mathrm{Hom}_{k'}(A\ ,\ \mathfrak{J}(Kk'))$. Décrivons ses composantes locales :

1° Si v se décompose dans k' ($v \in I$) $(\lambda_s\ ,\ 1)$.

2° Si v ne se décompose pas dans k' mais dans $k(+)$ ($v \in II_a$) (λ_{s+1}) .

3° Si v ne se décompose pas dans k' mais dans $k(-)$ ($v \in II_b$) $(\lambda_0\ \lambda_{s+1})$.

On renvoie pour les détails à l'article de POITOU [9].

2. Résolution générale.

On revient au problème du plongement diédral et quaternionien. D'après la partie précédente, on voit que le problème de plongement se traduit par l'une des deux situations suivantes.

(A) k est un corps local, χ est un générateur du groupe $A'(k)$ des caractères de A définis sur k .

(B) k est un corps de nombres ; on suppose les conditions locales vérifiées. χ est un élément non trivial du conoyau de π^*.

On notera C le groupe multiplicatif de $\bar{k}$ dans le cas local (A) et la limite inductive du groupe des classes d'idèles des extensions finies de k dans le cas (B), et $C(L)$ les points fixes de C par $\mathrm{Gal}(\bar{k}/L)$. Dans les deux cas, le problème de plongement est résoluble si, et seulement si, le cocycle $\chi^*(\varepsilon)$ de $H^2(G , C(K))$ est un cobord. C'est ce que l'on va expliciter dans ce paragraphe. On introduit les notations suivantes : Si G est le groupe diédral engendré par x et y ($x^{2^k} = 1$, $y^2 = 1$, $yxy^{-1} = x^{-1}$) , on note H le sous-groupe de G engendré par x , et k_0 l'extension de K/k laissée fixe par H. On a la suite exacte :

$$1 \longrightarrow H \longrightarrow G \longrightarrow g \longrightarrow 1 .$$

Elle induit une suite exacte de cohomologie

$$H^1(H , C(K)) \longrightarrow H^2(g , C(k_0)) \xrightarrow{\text{inf}} H^2(G , C(K)) \xrightarrow{\text{res}} H^2(H , C(K)) .$$

Or dans les deux cas envisagés, le groupe $H^1(H , C(K))$ est nul. Cela permet de traduire le fait que $\chi^*(\varepsilon)$ est nul. On obtient le lemme suivant.

LEMME 1. - *Soit* $X = \chi(\varepsilon)(x , x^{-1})$ *un représentant de la restriction de* $\chi^*(\varepsilon)$ *dans* $C(k_0)$ *et* $Y = \chi(\varepsilon)(y , y)$.

1° *Si* $\chi^*(\varepsilon)$ *est un cobord,* X *est une norme dans* $C(K)/C(k_0)$: $X = N_{K/k_0}(b)$. *De plus, il existe* c *appartenant à* $C(K)$ *et vérifiant* $c^x c^{-1} = b^{-1} b^{-xy}$.

2° $\chi^*(\varepsilon)$ *est un cobord si, et seulement si, on a :*

$$X \in N_{K/k_0}(C(K)) , \quad Yc^{-1} c^{-y} \in N_{k_0/k}(C(k_0)) .$$

Donnons quelques propriétés de X et Y.

LEMME 2. - X *est un élément de* $C(k_0)$ *de norme* 1 : $XX^y = 1$, Y *est un élément de* $C(k)$ *égal à* 1 *dans le cas du plongement diédral et à* $X^{2^{r-1}}$ *dans le cas du plongement quaternionien.*

THÉORÈME 3. - *Soit un élément* Z *de* $C(k_0)$ *vérifiant* $Z^y Z^{-1} = X$. *Dans le cas diédral ou dans le cas quaternionien, lorsque* Y *est norme d'un élément de* $C(k_0)$, *le problème de plongement a une solution si, et seulement si,* Z *est une norme d'un élément de* $C(K)$. *Dans le cas quaternionien, lorsque* Y *n'est pas norme d'un élément de* $C(k_0)$, *le problème de plongement a une solution si, et seulement si, le symbole de norme* $(Z , K/k_0)$ *est égal à* $x^{2^{k-1}}$.

Démonstration. - On étudie d'abord le cas diédral. Montrons que la condition donnée est suffisante. Pour cela, on vérifie que $\chi^*(\varepsilon)$ est un cobord à l'aide du lemme 1. Soit U un élément de $C(K)$ tel que $Z = N_{K/k_0}(U)$. On a $X = N_{K/k_0}(U^y/U)$. Donc X est une norme dans $C(K)/C(k_0)$. On peut alors prendre comme élément c vérifiant $c^x c^{-1} = (U^y/U)^{-1} (U^y/U)^{xy}$ l'élément $c = U^y/U$. On a alors trivialement

$$(Yc^{-1} c^{-y} , k_0/k) = 1 .$$

Donc $X^*(\varepsilon)$ est un cobord et le problème de plongement a une solution. Réciproquement, soit N une solution du problème. On a le lemme suivant.

LEMME 4. - *Si* N/k *est une extension diédrale, et si* a *est un élément de* $C(k)$, a *est une norme pour l'extension* N/k_0 .

Démonstration. - On a $(a , N/k_0) = \mathrm{Ver}(a , N/k)$, où Ver désigne le transfert de $\mathrm{Gal}(N/k)$ dans $\mathrm{Gal}(N/k_0)$. Le calcul de ce transfert montre qu'il est nul.

On applique ce lemme à $X^{2^{r-1}}$; on a donc

$$(X , N/k_0)^{2^{r-1}} = 1 .$$

Or $(X , N/k_0) = (Z/Z^y , N/k_0) = (Z , N/k_0)^2$. Donc $(Z , N/k_0)$ est d'ordre 2^r. Son image dans $\mathrm{Gal}(K/k_0) = H$ est égale à 1. Donc le symbole $(Z , K/k_0)$ est égal à 1, et Z est norme d'un élément de $C(K)$.

Le cas quaternionien se résoud en regardant comment il est lié au cas diédral (lemme 1) et en remarquant que les éléments X et Z sont les mêmes.

3. Plongement d'une extension p-adique.

On se place maintenant dans le cas (A), on commence par chercher le groupe $A'(k)$.

LEMME 5. - *Soit* q *l'entier défini ainsi :* 2^q *est l'ordre du sous-groupe des racines de l'unité d'ordre divisant* 2^r *de* k_0 *vérifiant* $\zeta^y = \zeta^{-1}$. *Alors* $A'(k)$ *est d'ordre* 2^q .

On note ζ une racine primitive d'ordre 2^q .

PROPOSITION 6. - *Soit* K/k *une extension diédrale de corps p-adiques,* k_0 *le corps quadratique de* k *laissé fixe par* x *, et* m *un élément de* k *vérifiant* $k_0 = k(\sqrt{m})$. *On définit l'élément* z *de* k_0 *par :*

$$z = 1 + \zeta \text{ si } q > 1 , \quad z = \sqrt{m} \text{ si } q = 1 .$$

Dans le cas du problème diédral, ou d'un problème quaternionien lorsque l'une des hypothèses suivantes est vérifiée :

(i) $q < r$;

(ii) $q = r$, $(-1 , k_0/k) = 1$,

le problème de plongement a une solution si, et seulement si, z *est norme d'un élément de* K . *Dans le cas quaternionien, lorsque* q *est égal à* r *et que* $(-1 , k_0/k)$ *est égal à* -1 , *le problème de plongement a une solution si, et seulement si, le symbole* $(z , K/k_0)$ *est égal à* $x^{2^{k-1}}$.

Dans le cas où k est une extension p-adique modérément ramifiée (p impair), on peut donner des conditions plus explicites.

PROPOSITION 7. - *Soit* K/k *une extension diédrale de corps* p*-adiques* $(p \neq 2)$. *Si* $r + k$ *est supérieur strictement à* 2, *le problème de plongement diédral (respectivement quaternionien) a une solution si, et seulement si,* k *ne contient pas les racines quatrièmes de l'unité,* μ_4, *et si* k_0 *contient les racines de l'unité d'ordre* 2^{r+k+1}. *Si* r *et* k *sont égaux à* 1, *le problème diédral (resp. quaternionien) a une solution si, et seulement si,* μ_4 *n'est pas inclus dans* k *mais dans* k_0 *(resp. n'est pas inclus dans* k *).*

4. Plongement d'une extension de corps de nombres.

Nous allons faire le plan d'étude de la résolution d'un tel problème.

1° Il faut d'abord trouver les conditions locales, et pour cela regarder tous les sous-groupes de décomposition. Lorsque le sous-groupe de décomposition est encore diédral, on peut appliquer les résultats du paragraphe 3. Les autres cas se résolvent facilement [3].

2° On doit ensuite regarder s'il y a une condition globale à écrire. Pour cela, on calcule l'extension $k(A')/k$. On obtient la proposition suivante.

PROPOSITION 8. - *L'extension* $k(A')/k$ *est cyclique dans les trois cas suivants :*

1° $r \leqslant 2$,

2° k *contient* $\eta + \eta^{-1}$, *où* η *est une racine de l'unité d'ordre* 2^r,

3° $K \cap k(\mu_{2^r}) = k_0$ *et* $\mathrm{Gal}(k(\mu_{2^r})/k_0)$ *ne contient pas* β *(élément agissant sur les racines de l'unité par* $\zeta \longrightarrow \zeta^{-1}$ *).*

Il y a une condition globale si, et seulement si, l'extension $k(A')/k$ *est non cyclique (de groupe de Galois engendré par* β *et* α^{2^s} *), et si toute place de* k *se décompose dans* $k(\sqrt{-m}, \zeta + \zeta^{-1})$ *où* ζ *est une racine de l'unité d'ordre* 2^{s+3}. *On rappelle que* m *est défini par* $k_0 = k(\sqrt{m})$.

Remarque. - Dans le cas où le corps de base k est $\mathbb{Q}$, supposons que m est choisi entier sans facteurs carrés. Il y a une condition globale si, et seulement si, m est différent de -1 et -2, si m est congru à -1 ou à -2 modulo 8, et si 2 est une norme dans $\mathbb{Q}(\sqrt{m})$.

La troisième partie consiste à se placer dans le cas où il existe une condition globale, et à la trouver explicitement. On obtient un représentant $\mathfrak{J}$ de la classe d'idèles $X = \psi(\varepsilon(x, x^{-1}))$, où ψ est l'élément du conoyau de π^* non nul (cf. § 2), par

$$\mathfrak{J} = \{(\zeta^2, 1)_{v \in I}, (\zeta)_{v \in II_a}, (i\zeta)_{v \in II_b}\},$$

où ζ désigne une racine de l'unité d'ordre 2^{s+3}. Un représentant de X appartenant à $\mathfrak{J}(k_0)$ et de norme 1 est, par exemple,

$$\mathfrak{J}_1 = a^{-1}(1 + \zeta^2)^{-1} \mathfrak{J} ,$$

où a est un élément de k_0 de norme $\zeta^2/(1 + \zeta^2)^2$. On a alors le théorème suivant.

THÉORÈME 9. - *Soit* U *un élément de* $\mathfrak{J}(k_0)$ *vérifiant* $U^y U^{-1} = \mathfrak{J}_1$. *Dans le cas diédral ou dans le cas quaternionien lorsque* $\sum_{v \in I} (-1 , k_0/k)_v$ *est égal à* 1, *ou que* s *est strictement inférieur à* $r - 3$, *le problème de plongement a une solution si, et seulement si,* U *est une norme d'un élément de* $\mathfrak{J}(K)$. *Dans le cas quaternionien,* $r = s - 3$, *et* $\sum_{v \in I} (-1 , k_0/k)_v = -1$, *le problème de plongement a une solution si, et seulement si, le symbole de norme* $(U , K/k_0)$ *est égal à* $x^{2^{k-1}}$.

Remarque. - Le calcul de U à partir de $\mathfrak{J}_1$ se fait facilement place par place. Par contre, le calcul explicite de $\mathfrak{J}_1$ demande de connaître un élément de $k(\sqrt{m})$ de norme $\zeta^2/(1 + \zeta^2)^2$. Par exemple, si le corps de base est $\underset{\sim}{Q}$, il s'agit de trouver un élément de norme 2. Cela est une question de tabulation. Connaissant cet élément, il est alors possible de donner la liste des entiers r pour lesquels K/k est plongeable dans une extension diédrale (resp. quaternionienne) d'ordre 2^{r+k+1}. Nous allons traiter rapidement un exemple.

Soit l'extension K/k, avec $k = \underset{\sim}{Q}(\sqrt{-1})$, $K = \underset{\sim}{Q}(\sqrt{-1} , \sqrt{31} , \sqrt{9118})$, $k_0 = \underset{\sim}{Q}(\sqrt{-1} , \sqrt{31})$. On a $d = 9118 = 2 \times 97 \times 47$.

1° *Conditions locales*. - Il suffit de regarder les places de k se ramifiant dans K ou divisant 2. Si $\mathfrak{P}$ divise 97 ou 47, $\mathfrak{P}$ se décompose dans k_0 ; la condition locale est alors que $k_{\mathfrak{P}}$ contienne les racines de l'unité d'ordre 2^{r+1}, c'est-à-dire que l'on ait $N\mathfrak{P} \equiv 1 \mod 2^{r+1}$. Or, $97 \equiv 1 \mod 2^5$; $47 \equiv -1 \mod 2^4$. Donc r doit être inférieur ou égal à 4. Si $\mathfrak{P}$ divise 31, comme k contient les racines quatrièmes de l'unité, $\mathfrak{P}$ doit se décomposer dans K (cf. paragraphe 3) et cela suffit. C'est le cas car $(d/31) = 1$. Si $\mathfrak{P}$ divise 2, $\mathfrak{P}$ se décompose dans k_0, et la condition locale est que les racines de l'unité qui sont contenues dans $k_{\mathfrak{P}}$ d'ordre divisant 2^r soient des normes de $K_{\mathfrak{P}}$, ce qui est vérifié : $(i , d)_{\mathfrak{P}} = (i , 2)_{\mathfrak{P}} (i , -1)^2_{\mathfrak{P}} = 1$.

En conclusion, les conditions locales sont vérifiées si, et seulement si, r est inférieur à 4.

2° On vérifie facilement qu'*il y a une condition globale à vérifier si* r *est supérieur ou égal à* 3.

3° On cherche cette condition globale. On a

$$\mathfrak{J}_1 = \frac{b}{1 + i} ((i , 1)_{v \in I} , (\zeta_8)_{v \in II_a} , (i\zeta_8)_{v \in II_b}) ,$$

avec ζ_8 une racine 8-ième de l'unité, et $b = 39 + 7\sqrt{31}$. On vérifie que seules interviennent dans $(U\ ,\ K/k_0)$ les places $\mathfrak{p}$ de k_0 divisant d. Comme toutes les places $\mathfrak{P}$ de k divisant d se décomposent dans k_0, on a

$$(U\ ,\ K/k_0) = \left(\frac{b}{1+i}\ ,\ d\right)_{\mathfrak{P}_{97}} \left(\frac{b}{1+i}\ ,\ d\right)_{\mathfrak{P}'_{97}} \left(\frac{b}{1+i}\ ,\ d\right)_{\mathfrak{P}_{47}} \left(\frac{b}{1+i}\ ,\ d\right)_{\mathfrak{P}_{2}} ,$$

où $\mathfrak{P}_p$ et $\mathfrak{P}'_p$ sont des prolongements de p à k. Un calcul facile montre que $(U\ ,\ K/k_0)$ est égal à 1. D'autre part, la quantité $\sum_{v\in I} (-1\ ,\ k_0/k)_v$ est égale à 1 $(k = \mathbb{Q}(\sqrt{-1}))$. On peut donc conclure :

L'extension $\mathbb{Q}(\sqrt{-1}\ ,\ \sqrt{31}\ ,\ \sqrt{9118})/\mathbb{Q}(\sqrt{-1})$ *est plongeable dans une extension diédrale (resp. quaternionienne) cyclique sur* $\mathbb{Q}(\sqrt{-1}\ ,\ \sqrt{31})$ *d'ordre* 8, 16, 32, 64, *et ne l'est pas pour des ordres supérieurs.*

BIBLIOGRAPHIE

[1] DAMEY (P.) et PAYAN (J.-J.). - Existence et construction des extensions galoisiennes non abéliennes de degré 8 d'un corps de caractéristique différente de 2, J. für die reine und angew. Math., t. 244, 1970, p. 37-82.

[2] DAMEY (P.) et MARTINET (J.). - Plongement d'une extension quadratique dans une extension quaternionienne, J. für die reine und angew. Math., t. 262-263, 1973, p. 323-338.

[3] GILLARD (R.). - Sur le problème du plongement des extensions galoisiennes, Thèse de troisième cycle, Grenoble, 1973.

[4] GILLARD (R.). - Plongement d'une extension d'ordre p ou p^2 dans une surextension non abélienne d'ordre p^3, J. für die reine und angew. Math., t. 268-269, 1974, p. 418-426.

[5] HALTER-KOCH (F.). - Construction of continuous idele class characters in quadratic number fields and embedding problems for dihedral and quaternion fields, Séminaire Delange-Pisot-Poitou : Théorie des Nombres, 17e année, 1975/76, n° 14, 13 p.

[6] HOECHSMANN (K.). - Zum Einbettungsproblem, J. für die reine und angew. Math., t. 229, 1968, p. 81-106.

[7] IKEDA (M.). - Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren, Abh. Math. Seminar Univ. Hamburg, t. 24, 1960, p. 126-131.

[8] NEUKIRCH (J.). - Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent. Math., Berlin, t. 21, 1973, p. 59-116.

[9] POITOU (G.). - Conditions globales pour les problèmes de plongement à noyau abélien, Annales Inst. Fourier, Grenoble (à paraître).

(Texte reçu le 19 juin 1978)

Bernadette PERRIN-RIOU
16 boulevard Colbert
92330 SCEAUX